Обухова В. О., РГППУ

ВОЗМОЖНОСТИ И УГРОЗЫ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Понятие «облачный сервис» обрело свою популярность сравнительно недавно, хотя появилось, а самое интересное, использовалось нами уже достаточно давно. Регистрируя адрес своей первой электронной почты, мы, сами того не подозревая, становились пользователями облачных сервисов.

Облачные (рассеяные) вычисления (англ. cloud computing, также используется термин «облачная (рассеянная) обработка данных») – технология обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Пользователь имеет доступ к собственным данным, но не может управлять и не должен заботиться об инфраструктуре, операционной системе и собственно программном обеспечении, с которым он работает. Термин «облако» используется как метафора, основанная на изображении Интернета на диаграмме компьютерной сети, или как образ сложной инфраструктуры, за которой скрываются все технические детали. Согласно стандартам Института инженеров по электротехнике и электронике (англ. Institute of Electrical and Electronics Engineers) – IEEE (I triple E – «Ай трипл и») – международной некоммерческой ассоциации специалистов в области разработки стандартов по радиоэлектронике и электротехнике, «облачная обработка данных – это парадигма, в рамках которой информация постоянно хранится на серверах в интернет и временно кэшируется на клиентской стороне, например, на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т. д.».

Данные хранятся в так называемых облачных хранилищах, это модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут располагаться удаленно друг от друга географически, вплоть до расположения на разных континентах[1].

Облачные технологии отвечают многим требованиям современного общества в основном таким как:

– самообслуживание по требованию, потребитель самостоятельно определяет и изменяет вычислительные потребности, такие как серверное время, ско-

[1] Что такое облачные технологии? URL: http://hostdb.ru/articles/show/id/47.

рости доступа и обработки данных, объем хранимых данных без взаимодействия с представителем поставщика услуг;

– универсальный доступ по сети, услуги доступны потребителям по сети передачи данных вне зависимости от используемого терминального устройства;

– эластичность, услуги могут быть предоставлены, расширены, сужены в любой момент времени, без дополнительных издержек на взаимодействие с поставщиком, как правило, в автоматическом режиме;

– учет потребления, поставщик услуг автоматически исчисляет потребленные ресурсы на определенном уровне абстракции (например, объем хранимых данных, пропускная способность, количество пользователей, количество транзакций), и на основе этих данных оценивает объем предоставленных потребителям услуг.

С точки зрения потребителя, эти характеристики позволяют получить услуги с высоким уровнем доступности (англ. high availability) и низкими рисками неработоспособности, обеспечить быстрое масштабирование вычислительной системы благодаря эластичности без необходимости создания, обслуживания и модернизации собственной аппаратной инфраструктуры.

Удобство, доступность и универсальность доступа обеспечивается широкой доступностью услуг и поддержкой различного класса терминальных устройств. Доступ к информации, хранящейся в облаке, может получить каждый, кто имеет компьютер, планшет, любое мобильное устройство, подключенное к сети Интернет. Из этого вытекает следующее преимущество – мобильность. У пользователя нет постоянной привязанности к одному рабочему месту, из любой точки мира менеджеры могут получать отчетность, а руководители – следить за производством.

Одним из важных преимуществ называют уменьшенную затратность, т. е. экономичность. Пользователю не надо покупать дорогостоящие, большие по вычислительной мощности компьютеры и программное обеспечение, а также он освобождается от необходимости нанимать специалиста по обслуживанию локальных IT-технологий.

Большие вычислительные мощности, которые предоставляются в распоряжение пользователя, которые можно использовать для хранения, анализа и обработки данных, обеспечивают высокую технологичность.

Некоторые эксперты утверждают, что надежность, которую обеспечивают современные облачные вычисления, гораздо выше, чем надежность локальных ресурсов, аргументируя это тем, что мало предприятий могут себе позволить приобрести и содержать полноценный ЦОД – специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.

Потребители облачных вычислений могут значительно уменьшить расходы на инфраструктуру информационных технологий (в краткосрочном и среднесрочном планах) и гибко реагировать на изменения вычислительных потребностей, используя свойства вычислительной эластичности облачных услуг[1].

На сегодняшний день недостаточно внимания уделяется вопросам информационной безопасности, когда речь заходит о новомодном, все более набирающем обороты ИТ-тренде – «облачных вычислениях». При этом к облачным сервисам обращается все больше и больше пользователей. Каковы же основные причины выбора, сделанного в пользу облаков? Ответ очевиден: в первую очередь, это экономичность и удобство пользования ими.

Пожалуй, самой масштабной проблемой, связанной с облачными вычислениями, является возможная утечка конфиденциальных данных. Однако решение у данной проблемы есть, но оно подходит далеко не всем. Повышение потенциальной сохранности данных возможно благодаря резервному копированию, но это существенно увеличивает расходы, что делает использование облачных технологий менее целесообразным.

Не менее тревожной перспективой для компаний, которые пользуются облачными услугами, является потеря собственных данных. Неважно, пропадут данные из-за технического сбоя, рядом с ЦОД окажется эпицентр землетрясения или информацию намеренно удалят злоумышленники – это может весьма плачевно закончиться для любой компании. Кроме того, шифрование данных в такой ситуации может усугубить ситуацию: утратить можно и ключ.

Нередко IT-администраторы всецело доверяют облачным интерфейсам для управления, настройки и мониторинга сервисов. Такие интерфейсы являются неотъемлемой частью облачных сервисов и предлагаются в качестве скелета. На их базе компании и третьи лица создают собственные решения, используя свои надстройки. Для этого различные облачные провайдеры или платформы выпускают собственные интерфейсы программирования приложений (иногда интерфейсы прикладного программирования, англ. application programming interface, API), которые и используются для создания надстроек. С точки зрения безопасности слоистая структура API представляет наибольший повод для беспокойства. Ведь зачастую доступ приходится предоставлять третьим лицам, выполняющим ту или иную часть работы.

[1] *Mell P., Grance T.* The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST, 2011. URL: http://csrc.nist.gov/publica–tions/nistpubs/800-145/SP800-145.pdf.

Руководителям организаций и их IT-отделов стоит реально понимать, какие последствия могут быть от перехода на облачные сервисы. Слабо проработанные интерфейсы и API могут оказаться ключом к тому, чтобы злоумышленники завладели вашей личной информацией или неограниченным доступом к вашим ресурсам.

Вредоносные инсайдеры всегда очень опасны: у них есть доступ и намерения не чисты. Это могут быть нынешние или бывшие сотрудники, подрядчики или партнеры по бизнесу – чем выше ранг, тем больше вреда они могут нанести. Заведомо неправильный сценарий может принести в облако хаос. Особенно просто это сделать, обладая внутренним доступом к администрированию. Злоупотребление возможностями облаков встречаются достаточно часто. Например, кто-то может воспользоваться вычислительными мощностями для того, чтобы взломать пароль к архиву. Или хакеры, которые с помощью тех же ресурсов производят DoS-атаку, рассылают спам или вредоносное ПО. Главная задача для облачных провайдеров – определить, какие случаи можно классифицировать как злоупотребления и разработать средства их идентификации[1].

И, наконец, с развитием облачных технологий особое беспокойство вызывает возможность вмешательства в личную жизнь пользователей услуг. Например, различным правительственным и другим структурам гораздо проще получить доступ к данным пользователя, хранящимся в облаке, нежели к данным, которые пользователь хранит локально. Такие примеры уже есть. Так, многие кредитные организации используют социальные сети как инструмент для поиска должников.

Учитывая все вышесказанное, необходимо помнить, что облачные технологии находятся на начальном этапе своего развития и их последующее распространение может стать одной из причин новых злоупотреблений и использования информации в корыстных целях. Поэтому на плечи провайдеров облачных сервисов ложится не только ответственность за предоставление бесперебойного доступа к услугам, но и защита данных клиентов, размещенных на удаленных серверах. На западе уже создаются организации, которые пытаются консолидировать и стандартизировать вопросы безопасности, связанные с облачными технологиями, например Cloud Security Alliance.

[1] Девять наиболее вероятных облачных угроз в 2013 г. URL: http://cloudzone.ru/articles/analytics/ 53.html.